PCT/NL 2004 / 000496

KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

Hierbij wordt verklaard, dat in Nederland op 8 juli 2003 onder nummer 1023861,
ten name van:

Pieter Gerard MACLAINE PONT

te Wijckel en

HOOGHEEMRAADSCHAP VAN RIJNLAND

te Leiden

een aanvrage om octrooi werd ingediend voor:

"DES virtueel stembiljet: Elektronisch netwerk verkiezingssysteem met virtueel stembiljet op basis van een symmetrisch cryptografisch algoritme, zoals DES, 3DES of AES",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 30 juli

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

Mw. D.L.M. Brouwer

1023861

Uittreksel

Het *DES virtueel stembiljet* systeem is een Elektronisch verkiezingssysteem, voor het houden van verkiezingen via openbare netwerken, op basis van een *virtueel stembiljet* dat met behulp van een symmetrisch cryptografisch algoritme (DES, 3DES of AES) wordt gecreëerd.

Iedere kiezer ontvangt vooraf een persoonlijke, geheime cryptografische sleutel Kp (of twee geheime waarden, waaruit na intikken zo'n sleutel kan worden berekend) en brengt zijn stem uit door daarmee de MAC te berekenen van de verkiezingsidentiteit en kandidaat van zijn keuze. Vooraf worden in een vertrouwelijk en besloten proces deze sleutels berekend en gereed gemaakt voor veilig transport en wordt een uitslag referentiebestand berekent, door voor iedere kiezer met diens Kp iedere mogelijk uit te brengen stem te berekenen en daarover een MDC berekening toe te passen. Dit uitslag referentiebestand wordt vooraf gepubliceerd.

De kiezer brengt zijn stem uit door zijn PC Internetbrowser, zijn smartcard of de SIM kaart in zijn GSM telefoon met zijn Kp een MAC te laten berekenen over de identiteiten van de verkiezing en zijn keuzekandidaat. Deze twee waarden vormen zijn *virtuele stembiljet* en worden door hem langs betrouwbare en vertrouwelijke weg bij het stembureau ingeleverd. Daar blijven alle virtuele stembiljetten vertrouwelijk tot na sluiting van de verkiezingen. Wel heeft ontvangstverificatie plaats. Ook per post kunnen eventueel Poststembiljetten worden ingezonden, die herleid kunnen worden tot een zelfde soort virtueel stembiljet.

Na afloop worden alle ontvangen virtuele stembiljetten gepubliceerd. Iedereen kan zelf de uitslag berekenen of kijken of zijn stem is meegeteld. Daarmee is een eenvoudig en betrouwbaar verkiezingssysteem mogelijk.

MullPon vof
Wijckel (F)

P.G.Maclaine Pont

2003-07-08

1023861

Indiening aanvrage om octrooi *DES virtueel stembiljet*

(versie 1.0)

Aanvrager (tevens uitvinder):

Maclaine Pont, Pieter Gerard; vennoot van MullPon vof.
Lynbaen 9
8563 AZ Wijckel
Nederland

Telefoon: 0621 233 982 Fax: 0514 605 945

Verdere aanvrager (alleen aanvrager):

Hoogheemraadschap van Rijnland
Bouwman, Simon
Archimedesweg 1
2333 CM Leiden
Nederland

Korte aanduiding

DES virtueel stembiljet: Elektronisch netwerk verkiezingssysteem met *virtueel stembiljet* op basis van DES, 3DES of AES.

Korte beschrijving

Elektronisch verkiezingssysteem, voor het houden van verkiezingen, referenda of belangrijke opinieonderzoeken via openbare netwerken, zoals Internet, digitaal telefonie of GSM netwerk, op basis van een *virtueel stembiljet* dat met behulp van een symmetrisch cryptografisch algoritme, zoals DES, 3DES of AES wordt gecreëerd. De belangrijkste beveiligingen en cryptografische bewerkingen voor de kiezer hangen

MullPon vof
Wijckel (F)

P.G.Maclaine Pont

2003-07-08

samen met de gebruikte techniek bij de verkiezing. Ze worden – al naar gelang - uitgevoerd door zijn Internet browser, de SIM-kaart in zijn GSM telefoon of een in zijn bezit zijnde smartcard.

5 Beschrijving

Het hier beschreven elektronisch verkiezingssysteem is een uitbreiding op door het door Herman Robers in december 1998 onder mijn leiding en begeleiding als afstudeerscriptie aan de Technische Universiteit Delft beschreven verkiezingsprotocol "Electronic elections employing DES smartcards".

Onder *verkiezing* of *verkiezingen* wordt hierna verstaan: een vorm van opinieonderzoek (zoals een openbare verkiezing voor een overheidslichaam of een referendum), waaraan alleen vooraf geregistreerde personen (*kiezers*) mogen deelnemen, waarbij hun opinie of keuze (hierna aangeduid als *stem*) gevraagd wordt uit vooraf volledig publiek gemaakte tekst (te kiezen kandidaten of referendumtekst, hierna aangeduid als *kandidatenlijst*), waarbij de door hun afgegeven stem vertrouwelijk is en vrijwillig kan worden ingediend gedurende een beperkt tijdsperiode (hierna aangeduid als *verkiezingsvenster*) bij een vooraf aangekondigde vertrouwde partij, waarbij iedere door een kiezer ingediende *stem* tenminste en maximaal éénmaal telt en waarbij de uitslag van het onderzoek publiek is en door onafhankelijke derden te controleren dient te zijn.

Een elektronisch verkiezingssysteem via een openbare netwerk is een systeem, dat een kiezer in staat stelt deel te nemen aan een verkiezing op een door hem zelf te kiezen plaats, van waaruit hij met de daartoe benodigde apparatuur via een openbaar netwerk zijn stem kan uitbrengen. Zo'n systeem zal hierna worden aangeduid als *elektronisch verkiezingssysteem*.

Bij een verkiezing met een elektronisch verkiezingssysteem onderscheiden we de volgende partijen en functies:

- Centrale verkiezingscommissie: een openbare, daartoe ingestelde partij, die de voor de elektronische verkiezingen noodzakelijke voorbereidingen treft, waaronder
  - De vaststelling en publicatie van een kiezersregister (waarin vastligt welke kiezers aan de verkiezing mogen deelnemen)
  - De vaststelling en publicatie van de informatie waarover de opinie of keuze van de kiezer gevraagd (de *kandidatenlijst*)
  - De organisatorische en technische voorbereiding van de elektronische verkiezingen, waaronder het voorzien van alle kiezers van specifieke informatie, die het hun mogelijk moet maken veilig en anoniem aan de elektronische verkiezingen deel te nemen, zoals bijvoorbeeld
    - Een document met een anonieme identiteit om aan deze verkiezing mee te mogen doen (zijn *Verkiezing Pseudo Identiteit* of *VPID*) en een geheim wachtwoord (*PW*) of
    - Een geheime, persoonlijke sleutel Kp voor iedere individuele kiezer, die op veilige wijze geladen wordt op diens smartcard of SIM-kaart van zijn GSM telefoon
    - De daartoe noodzakelijke regelingen en afspraken met derde partijen, zoals dienstverleners, telecommunicatiebedrijven en anderen
  - De vaststelling en publicatie van alle informatie die noodzakelijk is om op veilige en betrouwbare wijze het resultaat van de verkiezingen te kunnen vaststellen
- Kiezer (hiervoor reeds gedefinieerd), in het bezit van een instrument om aan de elektronische verkiezing mee te doen, zoals bijvoorbeeld:
  - Een document met een anonieme identiteit om aan deze verkiezing mee te mogen doen (zijn *Pseudo Verkiezing Identiteit* of *VPID*)
  - Een persoonlijke smartcard (zoals bijvoorbeeld zijn Studentenchipcard, een hem door de overheid verstrekte identiteit smartcard, of een hem door zijn bank verstrekte smartcard)
  - De smartcard (*SIM*) in zijn persoonlijke GSM telefoon
- Stem Unit (apparaat waarmee de kiezer zijn stem kan indienen, bijvoorbeeld:
  - Zijn PC met Internet browser

- Zijn PC met smartcardlezer
- Zijn GSM telefoon

- Stembureau (of wel de Stemverwerking centrale): de instantie waar de kiezer zijn stem via een netwerk moet indienen tijdens het *verkiezingsvenster*
- Toezichthoudend en controlerend orgaan: een openbaar en van de verkiezingen volledig onafhankelijk orgaan, belast met het toezicht op de verkiezing
- Terugvalsysteem: systeem dat in geval van een storing (of andere vorm van interruptie) die deelname door de kiezer aan de verkiezing onmogelijk maakt, deze toch in staat stelt op andere wijze (bijvoorbeeld per post) zijn stem uit te brengen.

Bij een verkiezing met een elektronisch verkiezingssysteem onderscheiden we de volgende fasen:

- Voorbereidingsfase
  - Centrale verkiezingscommissie stelt het volgende samen:
    - Verkiezingsnaam of –identiteit (ElID)
    - Kiezersregister (dat bevat de kiezers V1…Vn)
    - Publicatie daarvan en mogelijke aanpassingen door de kiezer
    - Kandidatenlijst (dat bevat de kandidaten C1…Cm)
    - Na vaststelling en bevriezing van kiezersregister en kandidatenlijst in een afgeschermd, vertrouwelijk proces:
      - Per kiezer de generatie van Kp of VPID en PW (in dat geval is Kp = functie {VPID, PW })
      - Berekenen van een veilig transportvorm van Kp (of VPID en PW) naar de kiezer
        - Ingeval Kp door cryptografische vercijfering onder een transportsleutel KEKt, die uitsluitend transport naar en laden van Kp in de smartcard of SIM van de kiezer mogelijk maakt
        - Ingeval VPID en PW door productie van een verzenddocument in gesloten enveloppe, waarbij

identiteit en adres van de kiezer alleen buiten op de enveloppe staat en VPID en PW, samen met algemene informatie over de verkiezing, zich binnen de enveloppe bevindt. Dit document kan eventueel dienen als stembiljet voor een terugvalsysteem per post; er wordt hierna aan gerefereerd als *Poststembiljet*. Op dit *Poststembiljet* zijn VPID, PW en ElID ook in machineleesbare vorm gecodeerd en is een lijst van alle kandidaten vermeld met de mogelijkheid er één als stem te kunnen markeren.

- Berekening van een uitslag referentiebestand en wel als volgt:
  - Voor iedere kiezer wordt een referentie uitslag berekend RnPotVote
  - Per kiezer n bestaat RnPotVote uit
    - Een kiezers referentie identiteit RnPID = MDC [DESmac (Kp, functie {ElID}]
    - Voor iedere kandidaat m uit de kandidatenlijst een referentie record RnCm = MDC [DESmac (Kp, functie {Cm, ElID}]
    - Transport naar buiten het afgeschermde, vertrouwelijke proces van
      - Het uitslag referentie bestand
      - De veilig transportvorm van Kp (of VPID en PW) voor transport naar de kiezer
    - Het wissen van alle vertrouwelijke, kiezersgerelateerde informatie (waaronder Kp (of VPID en PW)), dan wel opslag daarvan onder een uitsluitend

aan het Toezichthoudend en controlerend orgaan bekende cryptografische sleutel KEKctrl

- *MDC* staat voor een cryptografische hash functie, zoals de op DES gebaseerde Modification Detection Code
- *DES* staat voor een symmetrisch cryptografisch algoritme, zoals DES, 3DES of EAS
- *DESmac* staat voor een Message Authentication Code berekening met een symmetrisch cryptografisch algoritme, zoals de in ANSI gestandaardiseerde MAC met DES

- Het veilig verzenden van Kp of het Poststembiljet naar de juiste kiezer
- Publicatie (via een publiek netwerk) voor de start van de verkiezing van
  - De identiteit van de te houden verkiezing (ElID)
  - Het bevroren kiezersregister
  - De vastgestelde kandidatenlijst
  - Het referentie uitslagbestand RnPotVote voor alle kiezers
  - Bij gebruik van GSM telefoons: automatische installatie bij alle kiezers van de noodzakelijke extra functionaliteit voor stemberekening in hun GSM telefoon (m.b.v. SIM Tool Kit functionaliteit)
- De kiezer stelt (tijdig) vast of hij daadwerkelijk en correct in het kiezersregister is opgenomen, of hij vooraf de beschikking krijgt over de informatie (Kp of VPID en PW, de kandidatenlijst en de ElID) en middelen (afhankelijk van het geboden systeem: PC browser, smartcardlezer, smartcard, correcte versie SIM en GSM telefoon), noodzakelijk om aan de verkiezing deel te nemen

- Het Stembureau (of wel de Stemverwerking centrale) installeert een aantal netwerkservers om tijdens de verkiezingen de stem van iedere kiezer te kunnen ontvangen en wel zodanig, dat de toekomstige verbinding met de Stem Unit van iedere kiezer zal worden beschermd met SSL (of een vergelijkbare techniek bij gebruik van SMS via GSM telefoons), waarbij de kiezer eveneens eenduidig zal kunnen vaststellen werkelijk zijn stem bij het Stembureau in te leveren; tevens installeert het Stembureau het uitslag referentiebestand. Daarnaast voorziet het Stembureau in mogelijkheden om de belasting en het gebruik van het netwerk tussen de Stem Units van kiezers en het Stembureau te kunnen bewaken. Daarnaast installeert het Stembureau een aparte Stemontvangst bevestigingserver, die aan hetzelfde netwerk is verbonden en ook alleen via SSL toegang van kiezers toestaat.
- Het Toezichthoudend en controlerend orgaan controleert steekproefsgewijs en via klachtprocedures of de kiezer vooraf van de juiste informatie is voorzien
- Het Toezichthoudend en controlerend orgaan en ieder ander controleert of omvang en structuur van het referentie uitslagbestand overeenkomen met het kiezersregister en de kandidatenlijst

- Het verkiezingenvenster zelf
  - De kiezer (n) zelf
    - Stelt vast wat de identiteit van de verkiezing is (ElID)
    - Bepaald zijn keuze op grond van de publieke kandidatenlijst (Cx)
    - Maakt met zijn Stem Unit verbinding met het Stembureau
    - Overtuigd zich ervan dat aan de andere zijde van het netwerk werkelijk het stembureau aanwezig is en de verbinding is beveiligd (standaardfuncties van SSL)
    - Afhankelijk van zijn Stem Unit:
      - Bij een PC browser, al dan niet in combinatie met een smartcard: ontvangt automatisch als onderdeel van een normale webpagina de noodzakelijke functionaliteit voor het berekenen van zijn stem

- Bij een GSM telefoon: schakelt het vooraf ontvangen SIM Tool Kit programma in om deel te nemen aan deze verkiezing

- Geeft zijn keuze voor Cx aan zijn Stem Unit. Zijn Stem Unit berekent zijn stem, die uit de volgende twee elementen bestaat en zo samen zijn *virtuele stembiljet* vormen:
  - zijn kiezers identiteit VnPID = DESmac (Kp, functie {ElID}
  - zijn specifieke keuze voor kandidaat Cx: VnCx = DESmac (Kp, functie {Cx, ElID}
- Zorgt dat zijn Stem Unit zijn *virtuele stembiljet* daadwerkelijk doorgeeft aan het Stembureau door aanklikken van de juiste functie of intoetsen van de juiste toets
- Controleert of zijn virtuele stembiljet is aangekomen, door te kijken op de Stemontvangst bevestigingserver; is dat zo, dan is hij zeker dat zijn stem tijdig is uitgebracht (zijn stemunit berekent RnPID = MDC (VnPID), die weer gelijk is aan MDC [DESmac (Kp, functie {ElID}], en kijkt of dezelfde RnPID op de Stemontvangst bevestigingserver aanwezig is); hij bewaart een door de Stemontvangst bevestigingserver voor hem berekende kwitantie (Sign (Kconf, RnPID))
- Herhaalt bij twijfel of storingen van het proces of enig onderdeel daarvan zijn stemprocedure als hiervoor beschreven
- Stemt eventueel bij onmogelijkheid dit via het netwerk te doen per post met behulp van zijn *Poststembiljet*
- Weet, dat bij het meermalen indienen van zijn virtuele stembiljet deze als één telt als allen voor dezelfde kandidaat Cx zijn uitgebracht en als ongeldig als ze voor verschillende kandidaten zijn uitgebracht

o Stembureau (of wel de Stemverwerking centrale)
  - Vervult de rol in de communicatie met de kiezer als hiervoor beschreven

- Ontvangt ieder virtuele stembiljet als vertrouwelijke informatie, ontdoet deze van iedere tijd- en netwerkinformatie, berekent RnPID = MDC (VnPID), geeft RnPID door aan de Stemontvangst bevestigingserver en slaat het virtuele stembiljet zelf als vertrouwelijke informatie op in een vertrouwelijk Ontvangen Netwerk Stemmen bestand
- Zorgt dat de Stemontvangst bevestigingserver voortdurend alle ontvangen RnPID's na een (kort) tijdsinterval publiceert en kwiteert bij opvragen
- Verwerkt de (tijdig) binnengekomen Poststembiljetten met dezelfde berekening als die voor de elektronisch uitgebrachte stemmen, voegt deze poststemmen toe aan een vertrouwelijk Ontvangen Post Stemmen bestand

- Het Toezichthoudend en controlerend orgaan stelt vast of het Stembureau zijn taken correct vervult en bereikbaar is voor alle kiezers
- De Centrale verkiezingscommissie heeft geen specifieke taak tijdens het verkiezingsvenster zelf

- Uitslagfase
  - Het Stembureau (of wel de Stemverwerking centrale)
    - Sluit de toegang tot het Ontvangen Netwerk Stemmen bestand aan het eind van de verkiezingen en publiceert dit
    - Sluit de toegang tot het Ontvangen Post Stemmen bestand aan het eind van de verkiezingen of de tijdige inzendtermijn en publiceert dit
    - Publiceert statistische informatie over ontvangen stemmen, kiezers, RnPID's en Poststembiljetten
  - De Centrale verkiezingscommissie (en ieder ander)
    - berekent nu de uitslag als volgt:
      - Voegt alle stemmen in de Ontvangen Post Stemmen en Ontvangen Netwerk Stemmen bestanden bij elkaar en rekent al deze stemmen om naar Ontvangen Stem

referenties RnRecVote, door ieder virtuele stembiljet om te rekenen volgens de berekening RnRecVote = [MDC (VnPID)] // [MDC (VnCx)]

- Ontdubbelt (dezelfde RnPID en RnCx combinatie komt meerdere malen voor) en verwijdert ongeldige stemmen (twee of meer RnPID's met verschillende, op zich geldige RnCx combinatie's komen voor)
- Zoekt in het uitslag referentiebestand met RnRecVote de daar aanwezige RnPotVote gegevens op en bepaalt zo voor welke Kandidaat deze stem telt
  - Komen RnVID en/of RnCx van een RnRecVote niet voor in het uitslag referentiebestand, dan telt de stem niet mee
- Publiceert de verkiezingsuitslag en start daarmee de uitslag beroepstermijn (om kiezers en derden in staat te stellen de uitslag zelf te berekenen en daarna eventueel protest aan te tekenen)
- Ontvangt tijdens de uitslag beroepstermijn klachten van kiezers over door hun uitgebrachte stemmen die niet voorkomen in de Ontvangen Stemmen bestanden, terwijl ze wel over een geldige kwitantie van de stem bevestigingserver beschikken
- Verklaart de uitslag als correct na afloop van de uitslag beroepstermijn, indien geen geldige klachten zijn binnengekomen
- Verklaart de uitslag als ongeldig na afloop van de uitslag beroepstermijn, indien geldige klachten zijn binnengekomen (de verkiezingen zullen opnieuw moeten worden gehouden)

o De kiezer zelf controleert – desgewenst - of zijn stem, waarvoor hij een kwitantie heeft ontvangen, daadwerkelijk voorkomt in de gepubliceerde Ontvangen Stemmen bestanden; indien onjuist, dan dient hij een klacht in

- Derden en de kiezer zelf controleren de uitslagberekening met behulp van de gepubliceerde informatie; indien onjuist, dan dienen zij een klacht in.
- Het Toezichthoudend en controlerend orgaan
  - Controleert de berekeningen van het stembureau op correctheid en plausibiliteit
  - Controleert de juiste afwikkeling van de klachten tijdens de uitslag beroepstermijn
  - Verklaart op grond daarvan of een door de Centrale verkiezingscommissie correct bevonden uitslag ook daadwerkelijk bindend is.

Toevoegingen

- De Stemontvangst bevestigingserver maskeert de vraag van iedere kiezer om anonimiteit te garanderen: geeft groepen RnPID's op ieder verzoek i.p.v. één specifieke RnPID
- Test voor het verkiezingsvenster door de kiezer van zijn faciliteiten m.b.v. een teststem, te controleren door hemzelf met het vooraf gepubliceerde uitslag referentiebestand
- Asymmetrisch sleutelgebruik van geheime DES of 3DES transportsleutels en KEKctrl kan worden toegepast op basis van de Control Vector architectuur voor DES van IBM Corporation of een vergelijkbare oplossing. Daarmee kunnen risico's over het in verkeerde handen raken van Kp aanzienlijk worden beperkt en beheerst.

Conclusies

1. Relatief eenvoudig verkiezingssysteem, dat volledig is te realiseren binnen op dit moment op grote schaal aanwezige technische voorzieningen (Internet browsers, DES en 3DES smartcards, GSM telefoons met SIM kaarten die DES en 3DES berekeningen doen en eenvoudig met SIM Tool Kit van nieuwe functies kunnen worden voorzien).
2. Verkiezingsprotocol is gebaseerd op bekende, reeds gestandaardiseerde cryptografische functionaliteit (MAC en MDC) van een symmetrische algoritme. Door toepassing van deze functies op een andere wijze, dan tot nu voorzien, worden voor dit verkiezingsprotocol functies gecreëerd, waarvoor normaal publieke sleutel algoritmen toegepast zouden moeten worden. Aangezien de laatste technische faciliteiten vereisen, die grootteorden liggen boven die voor een symmetrisch algoritme, is toepassing daarvan binnen de huidige infrastructuren praktisch onmogelijk of ongewenst.
3. Door de eenvoudige opzet is het systeem geheel als "store-and-forward" systeem op te zetten (via SMS bij GSM telefoon of eenvoudige server contacten bij gebruik van Internet servers en clients). Daarmee is het systeem met eenvoudige middelen op grote schaal inzetbaar, is extra of reserve capaciteit eenvoudig te realiseren en is het systeem inherent ongevoelig voor aanvallen of allerlei vormen van misbruik.
4. Gestemd wordt met behulp van een *virtueel stembiljet*, dat alleen door de keizer zelf kan worden berekend. Het systeem is in staat meerdere *virtueel stembiljetten* van dezelfde kiezer als één stem te herkennen. Daarmee is het mogelijk om op eenvoudige wijze het systeem ongevoelig te maken voor storingen of interrupties en mag de kiezer bij twijfel zijn (zelfde) stem nogmaals uitbrengen, zelfs met een andere techniek als waarmee hij het de eerste maal deed.
5. Openbare controle op het verkiezingssysteem is (op grote schaal) mogelijk.
6. Er is een volledige scheiding tussen bij de verkiezing betrokken partijen, zoals die van organisator, stembureau, controleorgaan, kandidaat en kiezer.
7. Het systeem voldoet aan alle eisen, die daaraan bij verkiezingen voor overheidsorganen worden gesteld of kan daar op eenvoudige wijze aan voldoen.